

ORIGINAL

AO 106 (Rev. 04/10) Application for a Search Warrant (USAO CDCA Rev. 01/2013)

UNITED STATES DISTRICT COURT

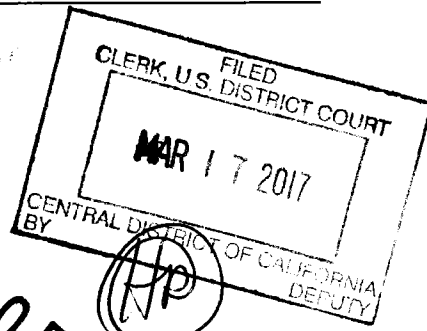
for the
Central District of California

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)A black Kyocera Cellphone, Bearing IMEI
014016001882356; and a Black Motorola Cellphone,
Bearing FCC ID IHDP56ME1;
Seized from GERSIO LOPEZ on January 29, 2017

Case No.

17MJ00596



APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Central District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 1708, 371, 1344, 1028, 1029 and 1028A

Offense Description
See attached Affidavit.

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

LOGGED

2017 MAR 17 AM 11:44
CLERK, U.S. DISTRICT COURT
CENTRAL DISTRICT OF CALIF.
LOS ANGELES
COW

Sworn to before me and signed in my presence.

Date:

3/17/17

City and state: Los Angeles, California

Applicant's signature

Kimberly Granger, USPI Postal Inspector

Printed name and title

Judge's signature

Hon. Jacqueline Chooljian, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

DEVICES TO BE SEARCHED

The following digital devices, seized by the Sierra Madre Police Department on or about January 29, 2017, and currently in the possession of the United States Postal Inspection Service in Pasadena, California:

1. A black Kyocera cell phone, bearing IMEI 014016001882356; and
2. A black Motorola cell phone, bearing FCC ID IHDP56ME1.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are the fruits, instrumentalities, and evidence of 18 U.S.C. § 1708 (Mail Theft and Possession of Stolen Mail), 18 U.S.C. § 371 (Conspiracy), 18 U.S.C. § 1344 (Bank Fraud), 18 U.S.C. § 1028 (Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information), 18 U.S.C. § 1029 (Access Device Fraud), and 18 U.S.C. § 1028A (Aggravated Identity Theft), namely:

a. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show address book information, including all stored or saved telephone numbers;

b. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of LOPEZ'S PHONES and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

c. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device;

d. Records, documents, programs, applications,

photographs, screenshots, images, or materials relating to mail, mail matter (whether opened or unopened), and/or access devices, including credit cards, debit cards, gift cards, bank accounts, or other financial institution accounts;

e. Data, records, documents, or information (including e-mails and messages) pertaining to obtaining, possessing, using, or transferring personal and/or financial transaction identification information for persons other than GERSIO A. LOPEZ ("LOPEZ"), such as names, addresses, phone numbers, credit and debit card numbers, security codes, bank account and other financial institution account numbers, Social Security numbers, email addresses, IP addresses, as well as PIN numbers and passwords for financial institutions or internet service providers;

f. Records, documents, programs, applications, or materials pertaining to applications for, or use of, credit or debit cards, bank accounts, or merchant processor accounts;

g. Data, records, documents (including e-mails), or information reflecting or referencing purchases of merchandise, securities, electronic currency, and other valuable things;

h. Software, devices, or tools used to obtain, create, or use counterfeit or unauthorized checks, coupons, or access devices such as credit, debit, bank, and gift cards;

i. Any documents or records relating to any bank accounts, credit card accounts, or other financial accounts of any individual who is not LOPEZ;

j. Records, documents, programs, applications, or materials relating to United States mail or mail matter that is not addressed to LOPEZ;

k. The content of any calendar or date book stored on any of LOPEZ'S PHONES;

l. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

m. Any device used to facilitate the above-listed violations (and forensic copies thereof).

2. With respect to any of LOPEZ'S PHONES used to facilitate the above-listed violations containing evidence falling within the scope of the foregoing categories of items to be seized:

a. Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

b. Evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. Evidence of the attachment of other devices;

- d. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;
- e. Evidence of the times the device was used;
- f. Passwords, encryption keys, and other access devices that may be necessary to access the device;
- g. Applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;
- h. Records of or information about Internet Protocol addresses used by the device;
- i. Records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

3. In searching the devices listed in Attachment A (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

- a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any device capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each device where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the devices as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. If additional time is needed, the government may seek an extension of this time period from the Court on or before the date by which the search was to have been completed.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool

Kit), which tools may use hashing and other sophisticated techniques.

e. If the search team, while searching a device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

f. If the search determines that a device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

g. If the search determines that a device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the device but may not access them (after the time for searching the device has expired) absent further court order.

i. The government may retain a device itself until further order of the Court or one year after the conclusion of the criminal investigation or case (whichever is latest), only

if the device is determined to be an instrumentality of an offense under investigation or] the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending). Otherwise, the government must return the device.

j. Notwithstanding the above, after the completion of the search of the devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

4. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Kimberly Granger, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against and an arrest warrant for GERSIO AMIMAELO LOPEZ ("LOPEZ") for a violation of Title 18, United States Code, Section 1708 (Possession of Stolen Mail).

2. This affidavit is also made in support of an application for a warrant to search the following two digital devices seized on January 29, 2017, from LOPEZ and currently in the possession of the United States Postal Inspection Service ("USPIS") in Pasadena, California, as described more fully in Attachment A, which is incorporated by reference:

a. A black Kyocera cellphone, bearing IMEI 014016001882356 ("LOPEZ'S PHONE 1"); and

b. A black Motorola cellphone, bearing FCC ID IHDP56ME1 ("LOPEZ'S PHONE 2") (collectively, "LOPEZ'S PHONES").

The requested search warrant seeks authorization to seize evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1708 (Mail Theft and Possession of Stolen Mail), 371 (Conspiracy), 1028 (Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information), 1029 (Access Device Fraud), 1344 (Bank Fraud), and 1028A (Aggravated Identity Theft), as described further in Attachment B, which is also incorporated by reference.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested criminal complaint, arrest warrant, and search warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND OF POSTAL INSPECTOR KIMBERLY GRANGER

4. I am a Postal Inspector with USPIS and have been so employed since July 2014. I am currently assigned to the Los Angeles Division, Pasadena Mail Theft Team, where my responsibilities include the investigation of crimes against the United States Postal Service ("USPS") and crimes related to the misuse and attack of the mail system, including theft of United States mail, possession of stolen mail, fraud, access device fraud (including credit and debit cards), and identity theft. I completed a twelve-week basic training course in Potomac, Maryland. That course included training in the investigation of identity theft via the United States Mail.

5. I also investigate crimes related to the use, theft, or counterfeiting of USPS postal keys (referred to as "arrow keys") and locks. From my training and experience, I know that USPS arrow keys are keys used by mail carriers to unlock USPS arrow locks, in order to gain access to neighborhood delivery

collection box units, housing complexes or apartment buildings and deliver mail to the respective mailboxes found inside – most commonly found in a mailbox panel. Postal arrow keys are also sometimes used to gain access to mail collection boxes in a specific area. A postal arrow key is not for use by, or available to, the general public.

III. SUMMARY OF PROBABLE CAUSE

6. On January 29, 2017, at approximately 9:46 p.m., while on uniformed patrol in Sierra Madre, California, Sierra Madre Police Department ("SMPD") Officer Raymond So conducted a traffic enforcement stop of LOPEZ for failure to stop. Officer So discovered that LOPEZ had an expired driver's license. Officer So then asked LOPEZ if he could search LOPEZ's car and person. LOPEZ gave consent. Officer So found a 2- to 3-inch clear glass smoking pipe with white and brown substance on LOPEZ. SMPD Officers recovered from LOPEZ's car approximately 57 pieces of mail, four check books, 19 checks, five access devices, and three U.S. passports, all in names other than LOPEZ.

IV. STATEMENT OF PROBABLE CAUSE

A. Sierra Madre Department Arrest

7. Based on my conversations with Sergeant Henry Amos and Officer Raymond So, as well as my review of SMPD reports, I know the following:

a. On January 29, 2017, at approximately 9:46 p.m., Officer So was on uniformed patrol in a marked black and white patrol car parked on Baldwin Avenue north of Orange Grove Avenue

in Sierra Madre, California. Officer So saw a black Kia Forte, bearing California License Plate 7SLR473, not make a complete stop while going eastbound on Orange Grove Avenue at Baldwin Avenue, a violation of California Vehicle Code 22450(a). Officer So conducted a traffic stop and approached the driver, LOPEZ, who was the sole occupant of the car.¹ Officer So was wearing a body-worn video camera.

b. Officer So asked LOPEZ for his driver's license, vehicle registration, and proof of insurance.² LOPEZ said he had a license but it was expired, in violation of California Vehicle Code Section 12500(a). Officer So conducted a records check which revealed that LOPEZ had an expired license and the car's registration had expired on August 3, 2016.

c. Officer So asked LOPEZ where he was coming from and LOPEZ said he was coming from his aunt's house in Pasadena. LOPEZ could not provide the address for his aunt's house. LOPEZ appeared very nervous and had trouble finding his driver's license, vehicle registration, and proof of insurance. Sergeant Ruben Enriquez and Officer Thomas Onderdonk arrived on scene to assist.

d. Officer So asked LOPEZ if he could conduct a search of the car and his person, and LOPEZ said yes. Officer So asked LOPEZ to step out of the car. Officer So then

¹ On March 3, 2017, I conducted a Department of Motor Vehicle ("DMV") records check which revealed the car is registered to LOPEZ.

² When I spoke with Officer So, I learned that he is fluent in Spanish and that the recorded conversation between him and LOPEZ were in Spanish.

conducted a search of LOPEZ and recovered a 2- to 3-inch clear glass smoking pipe with a bulbous end. The bulbous end contained a white and brown substance. Officer So believed that the substance was an illicit drug and the pipe had been used to ingest the drug, a violation of Health and Safety Code Section 11364.1(a). Officer So continued his search of LOPEZ and found a gas torch lighter and a small LED flashlight. Officer So asked LOPEZ what these items were used for, but LOPEZ did not answer his questions. Officer So then handcuffed LOPEZ and told him he was only being detained, not under arrest. Officer So placed LOPEZ in the back of his patrol unit.

e. SMPD Officers began a search of the car. Officer So looked in the driver's side door panel and found a small black and white pouch with a white substance, which appeared to be methamphetamine, in violation of Health and Safety Code Section 11377(a).³ Sergeant Enriquez asked LOPEZ what was inside the plastic pouch and LOPEZ did not answer.

f. Officer So searched the back seat of the car and found multiple pieces of mail addressed to different cities in California, including the city of Sierra Madre. The mail did not bear LOPEZ's name and was addressed to other individuals. Officer So searched the glove box and trunk of the car and found more mail in names other than LOPEZ. In total, there was mail from twelve different cities addressed to different residents in

³ Officer So tested the substance later and the results showed that it was methamphetamine and weighed about 0.1 grams.

each city. Sergeant Enriquez asked LOPEZ who the mail belonged to and LOPEZ did not answer.

g. Officer So also recovered three passports that belonged to two different individuals, K.C. and S.R., and checks in names other than LOPEZ. After finding the stolen documents, Officer So formed the opinion that LOPEZ used the flashlight found on his person to look through people's mailboxes and steal mail from inside, as there is no street lighting on Orange Grove Avenue and Manzanita Avenue, from where several of the mail matters were stolen.

h. Officer So told LOPEZ he was under arrest and transported LOPEZ to the Pasadena Jail for booking. Officer So read LOPEZ his Miranda rights from his department issued card. LOPEZ did not want to answer any questions and requested an attorney. Officer So did not ask LOPEZ any more questions.

B. USPIS Evidence Review

8. On February 3, 2017, I met Sergeant Amos and took possession of the evidence recovered from LOPEZ. Based on my review of the evidence, I know LOPEZ possessed approximately 57 pieces of mail, four check books, 19 checks, five access devices, and three U.S. passports, in names other than LOPEZ. LOPEZ was also in possession of LOPEZ'S PHONES.

V. TRAINING AND EXPERIENCE REGARDING MAIL AND IDENTITY THEFT

9. Based on my training and experience, including being a member of a USPIS Mail Theft Team, and information obtained from other law enforcement officers who investigate mail and identity theft, I know the following:

a. Persons who steal mail are often involved in fraud and identity theft crimes. These individuals usually steal mail looking for checks, access devices, other personal identifying information (such as names, Social Security numbers, and dates of birth), and identification documents that they can use to fraudulently obtain money and items of value. Mail thieves often retain these items of value from stolen mail in order to make fraudulent purchases or sell the items to others in exchange for cash or drugs.

b. Persons involved in mail theft and identity fraud typically obtain checks, access devices, and personal identifying information by stealing the mail of victims, or from co-conspirators who have done these things.

c. It is common practice for individuals involved in mail theft, identity theft, bank fraud, and access device fraud crimes to use and maintain digital devices. Such digital devices are often used to facilitate, conduct, and track their fraudulent transactions and identity theft. Suspects often use digital devices to perpetrate their crimes due to the relative anonymity gained by conducting financial transactions electronically or over the Internet. They often employ digital devices for the purposes, among others, of: (1) applying online for fraudulent credit cards; (2) obtaining or storing personal identification information for the purpose of establishing or modifying fraudulent bank accounts and/or credit card accounts; (3) using fraudulently obtained bank accounts and/or credit card accounts to make purchases, sometimes of further personal

information; (4) keeping records of their crimes; (5) researching personal information, such as social security numbers and dates of birth, for potential identity theft victims; and (6) verifying the status of stolen access devices.

d. Often times mail and identity thieves take pictures of items retrieved from stolen mail or mail matter with their cellphones. It is also common for these individuals to use digital devices to store information about their identity theft crimes during and long after the crimes have been committed. This information can include: logs of fraudulent transaction history; records of funds received; information regarding individuals and companies that have been victimized; records of payments from co-conspirators; and victim "profiles." Such "profiles" contain the personal identifying information of victims, such as names, Social Security numbers, dates of birth, driver's license or state identification numbers, alien registration numbers, passport numbers, and employer or taxpayer identification numbers.

e. It is common for mail thieves, identity thieves, and individuals engaged in bank fraud, access device fraud and identification document fraud to use equipment and software to print credit and identification cards, to create magnetic strips for credit cards, to use embossing machines to create credit cards, to use laser printers to create checks, and to use magnetic card readers to read and re-encode credit cards. Software relevant to such schemes can often be found on digital devices.

f. Based on my training and experience, I know that individuals who participate in mail theft, identity theft, bank fraud, and access device fraud schemes often maintain telephone numbers, email addresses, and other contact information and communications involving their co-conspirators in order to conduct their business. Often times, they do so on their digital devices. Suspects often use their digital devices to communicate with co-conspirators by telephone, e-mail, text messages, and social media.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

10. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that it is not always possible to search digital devices for digital data in a single day or even over several weeks for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it takes time to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the type of digital device, operating system, and software application being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise,

scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. It is difficult to estimate the precise storage space contained on the digital devices listed in Attachment A before conducting a preliminary examination of the device, but, based on my training and experience, I know that cellular telephones can contain multiple gigabytes of storage space. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an

active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image

as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone


else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

11. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. CONCLUSION

For all the reasons described above, there is probable cause to believe that LOPEZ violated Title 18, United States Code, Section 1708 (Possession of Stolen Mail). Based on the foregoing facts, I believe there is also probable cause to believe the items listed in Attachment B, which constitutes evidence, fruits, and instrumentalities of violations of the offenses described above will be found on the devices described in Attachment A.



KIMBERLY GRANGER
United States Postal Inspector,
United States Postal Inspection
Service

Subscribed to and sworn before me
this 17 day of March 2017.



HONORABLE JACQUELINE CHOOLJIAN
UNITED STATES MAGISTRATE JUDGE